Exhibit 1-G

Data Security Services

Contract Work Authorization (CWA)

This Contract Work Authorization ("CWA") No. C14373 is issued under and pursuant to the Blanket Agreement or Master Service Agreement No. C73 (fka 4400011340) dated January 19, 2017 (the "MSA") between the below-named Contractor ("Contractor"), a Delaware Limited Liability Partnership and Pacific Gas and Electric Company ("PG&E"), a California corporation with its headquarters located at 77 Beale Street, San Francisco, California 94105. Contractor shall perform all Work under this CWA pursuant to and in accordance with the terms and conditions of the MSA.

Contractor's Legal Name:	KPMG LLP	**Total Number of Pages: 27**
Contractor's Address:	P.O. BOX 120001 DALLAS, TX 75312	
Project Name:	Data Security Program 2019/2020 Roadmap Implementation Support	
Job Location:	Approved PGE Locations	

WORK: Contractor shall, at its own risk and expense, perform the Work described in this Contract Work Authorization and furnish all labor, equipment, and materials necessary to complete the Work as summarized below and as more fully described in Attachment 1, Scope of Work. A high-level description of Contractor's services during the project period of performance includes:

- Perform data security inventory, dashboard, and remediation efforts for PG&E's on premise unstructured data (2019) and cloud environments (2020). This effort also includes PG&E onboarding Collibra, a data governance and inventory tool, for use by the program to track these tasks.
- Develop policies within PG&E's current Data Loss Protection (DLP) platform (Symantec DLP) that will detect PG&E's most sensitive data (Confidential and Restricted data) stored within identified on premise unstructured data repositories.
- Assist with expansion of the current DLP system's capabilities into the PG&E cloud environment. Contractor will perform an evaluation of key capabilities required in order to deploy an effective DLP capability in PG&E's cloud environment and recommend policies and supporting technologies required to enable active monitoring and blocking capabilities.
- Perform tasks related to introduction of PG&E's selected de-identification tool into PG&E test and production environments and support the configuration of the technology to de-identify on premise unstructured data (2019) and cloud environments (2020).

ATTACHMENTS: Each of the following documents are attached to this CWA and are incorporated herein by this reference:
Attachment 1: Scope of Work, pages 3-24
Attachment 2: Appendix A pages 25-27

CWA TERM:	This CWA is effective upon signature by both parties and expires on December 21, 2020. Time is of the essence.
CWA COMPLETION:	Contractor shall commence performance hereof when directed to do so by PG&E and Work shall be completed by the completion date of December 21, 2020.

CONSIDERATION: As full consideration for satisfactory performance of the Work under this CWA by Contractor, PG&E's total obligation to Contractor shall not exceed the following amount. This amount is inclusive of all taxes incurred in the performance of the Work. Any change to this amount shall only be authorized in writing by a PG&E CWA Change Order, fully executed by both PG&E and Contractor.

TOTAL: **$ 2,705,013.50 (***fixed fee services ($2,362,456.50 + expenses $342,557***)**

THE PARTIES, BY SIGNATURE OF THEIR AUTHORIZED REPRESENTATIVES, HEREBY AGREE TO THE TERMS OF THIS CONTRACT WORK AUTHORIZATION.

PG&E Corporation ("PG&E Corp.") and Pacific Gas and Electric Company (the "Utility," and, together with PG&E Corp., the "Debtors"), are debtors-in-possession in a proceeding pending under chapter 11 of title 11 of the United States Code (the "Bankruptcy Code"), in the United States Bankruptcy Court for the Northern District of California. Nothing herein shall be deemed to constitute an assumption of the Contract and/or any CWA or a waiver or modification of the Debtors' rights to assume, assume and assign, or reject the Contract and/or any CWA pursuant to section 365 of the Bankruptcy Code. The Debtors hereby reserve all rights available to them under such proceedings. Any amounts paid by the Debtors hereunder must be applied to goods and/or services provided to the Debtors on or after January 29, 2019 (the "Petition Date") and shall not be applied to satisfy Claims (as defined in the Bankruptcy Code) arising prior to the Petition Date

PACIFIC GAS AND ELECTRIC COMPANY		**CONTRACTOR: KPMG LLP**	
Signature	DocuSigned by: Larry Hernandez A1577063EB7B41E...	**Signature**	DocuSigned by: Michael Gomez 6982A1552B97492...
Name	Larry Hernandez	**Name**	Michael Gomez
Title	Manager, Sourcing Operations	**Title**	
Date	3/20/2019	**Date**	3/20/2019

Contract Work Authorization

ADMINISTRATION			
PG&E Negotiator	Steve Murley	**Contractor Represent**	Michael Gomez
Phone	415-973-5215	**Phone**	Cell: (202) 999-9383
Email	S6M4@pge.com	**Email**	michaelgomez@KPMG.com
Accounting Reference			
PG&E Work Supervisor:		**Phone:**	
INVOICE INSTRUCTIONS: As described in more detail in the Invoicing section of the Terms and Conditions, Contractor shall send invoices for each payment when due, showing the Purchase Order Number (starts with "27" or "35") and the Line Item number, if applicable.	The default submission system for invoices to PACIFIC GAS AND ELECTRIC COMPANY should be through the Taulia electronic invoicing portal, which also provides real-time invoice payment status. In rare cases that it is infeasible for a supplier to use this system, please send paper invoices to the address below. Invoice payment status for paper invoices can be accessed through the automated PG&E Paid Help Line at (800) 756-PAID (7243) or by emailing APPaidline@pge.com		
	Send ORIGINAL Invoice to:	PG&E Accounts Payable* PO Box 7760 San Francisco, CA 94120-7760	
	Send COPY of Invoice to:	NA	

INTERNAL PG&E USE ONLY		
Distribution Date		
Distribution of Copies:	☒ ARIBA Contracts (CXXXX series): Buyer uploads an executed copy in Ariba.	☒ Contractor (Signed Original Copy)
	☒ Work Supervisor	☐ Manager
	☐ Invoice Approver	☐ Supervisor
	☐ V.P.	☐ Sourcing/ Purchasing
	☐ Director	☐ Law

Attachment 1- Statement of Work
Data Security Program 2019/2020 Roadmap Implementation Support

This Statement of Work (SOW) outlines the engagement between Pacific Gas and Electric Company ("PG&E" or "Client") with KPMG LLP ("KPMG" or "Contractor") to perform the services described below.

The governing Master Services Agreement for this work is #4400011340, executed January 19, 2017 and supersedes all other oral and written representations, understandings, or agreements relating to the subject matter hereof, as amended and as supplemented by the Systems Implementation Addendum in Appendix A.

1. Description of Services

This SOW includes work activities that continue the process of supporting PG&E build a data security program office (DSPO) at PG&E. The period of performance for this SOW and associated projects is during calendar years 2019 and 2020.

A high-level description of Contractor's services during the project period of performance includes:

- Perform data security inventory, dashboard, and remediation efforts for PG&E's on premise unstructured data (2019) and cloud environments (2020). This effort also includes PG&E onboarding Collibra, a data governance and inventory tool, for use by the program to track these tasks.

- Develop policies within PG&E's current Data Loss Protection (DLP) platform (Symantec DLP) that will detect PG&E's most sensitive data (Confidential and Restricted data) stored within identified on premise unstructured data repositories.

- Assist with expansion of the current DLP system's capabilities into the PG&E cloud environment. Contractor will perform an evaluation of key capabilities required in order to deploy an effective DLP capability in PG&E's cloud environment, and recommend policies and supporting technologies required to enable active monitoring and blocking capabilities.

- Perform tasks related to introduction of PG&E's selected de-identification tool into PG&E test and production environments, and support the configuration of the technology to de-identify on premise unstructured data (2019) and cloud environments (2020).

2. Scope

The scope of this engagement shall be limited to support those activities that are aligned to the 2019 and 2020 objectives of PG&E's DSPO, as outlined in this SOW, below. However, if changes are required, KPMG will work diligently with PG&E to document these changes in a change order or memo of understanding, as agreed between the parties.

3. Approach

Contractor's approach to maximizing efficiency and effectiveness of the engagement is through conducting multiple work streams concurrently, and building on foundational phases. (See Section 4 *Project Timelines* for further information.) To successfully complete these work streams in a timely manner, Contractor will maintain regular and open communication and close collaboration with PG&E program leads. Contractor will actively perform project management throughout the engagement duration including regular program status meetings and other milestones.

Project 1 – Data Security Inventory, Dashboard, and Remediation for Unstructured Data (2019) and Cloud Environments (2020)

This scope of this project is inventorying on premise unstructured (2019), which includes semi-structured, and cloud-based (2020) data repositories and advising on the re-configuration of PG&E's existing Collibra instance to track these repositories and provide program metrics around repository tracking activities.

This project will help achieve these goals by performing the following:

- Inventory the data environment by identifying PG&E data repositories (on premise unstructured in 2019 and cloud in 2020).
- Catalog discovered repositories (on premise structured and unstructured in 2019 and cloud in 2020) into the Collibra platform.
- Review repository characteristics to build a risk profile and identify critical gaps/risks
- Document capability gaps into a remediation and capability backlog

The table below summarizes our anticipated phases, activities and deliverables for Project 1:

PROJECT 1		
Phase	**Activities**	**Deliverables**
Inventory Data Environment	— Revise project scope and charter, project work plan, and project job estimate — Revise data inventory template — Select business processes that will be in-scope for discovery efforts based off the PG&E data governance team's data domain model — Collaborate with Privacy and LOBs to define Restricted and Confidential data elements for documentation within data inventory. — Conduct top-down data inventory exercise in scope data assets (on premise unstructured in 2019 and cloud in 2020): — Perform stakeholder interviews to understand business processes and review existing process documentation and identify Restricted and Confidential data assets in use — Socialize populated data inventory with stakeholders	— Revised project scope and charter, project work plan, and project job estimate — Populated data inventory with associated data classification and extract of data inventory documented in Collibra for structured and unstructured data (2019), cloud data (2020)
Support Configuration of Collibra	— Draft the following PG&E ITM project deliverables using PG&E ITM templates:	— Change engagement plan

PROJECT 1		
Phase	**Activities**	**Deliverables**
and onboard repositories	• Change engagement plan that uses PG&E template • Collibra use cases and requirements documentation • Configuration management plan • Disaster recovery plan — Assist PG&E Collibra support team to configure Collibra for maintaining on premise structured and unstructured data in 2019, and cloud-based inventories in 2020 — Draft the following documentation: • Data inventory maintenance playbook • Data inventory remediation playbook • Requirements for connector from Collibra to Brinqa, PG&E's implemented cyber risk intelligence and analytics platform — Assist the PG&E Brinqa team to create a unified Brinqa view showing data repositories (structured, unstructured, and cloud), the Confidential and Restricted data stored within these repositories, and the protections in place to protect this data (2020) — Populate Collibra with inventory data (2018 on premise structured data, 2019 on premise unstructured data, 2020 cloud-based data) — Test the new functionality of the Collibra tool and the data inventory remediation playbook by conducting the following activities: • Perform a data security gap assessment that identifies and prioritizes data security risks for a minimum of ten (10) repositories (2019 on premise unstructured data, 2020 cloud data) • Leverage data security gap assessment to collaboratively select and agree two to four (2-4) production repositories to remediate using currently installed PG&E tools and following the data inventory remediation playbook • Draft detailed remediation work plans and recommendations for the remediation of two to four (2-4) production repositories • Pilot remediation of two to four (2-4) production repositories • Support and PG&E team in the test/pilot remediation of two to four (2-4) repositories	— Collibra use cases and requirements document — Configuration management plan — Disaster recovery plan — Data inventory maintenance playbook and data remediation playbook — Performance test plan — Data security gap assessment for minimum 10 repositories (on premise unstructured data, 2019; cloud 2020) — Detailed remediation work plans for two to four (2-4) repositories (on premise unstructured data, 2019; cloud 2020) — Two to four (2-4) repositories remediated in pilot (on premise unstructured data, 2019; cloud 2020) — Updated data inventory remediation playbook (on premise unstructured data, 2019; cloud 2020) — Test results and disaster recovery exercise report

PROJECT 1		
Phase	**Activities**	**Deliverables**
	• Update data inventory remediation playbook based on observations obtained during the test/pilot remediation activities	
Support configuration of the data security dashboard in Collibra	— Establish a dashboard view to monitor program metrics, inventory gaps, and remediation activity progress in Collibra — Generate Collibra run book (included in the maintenance playbook) — Draft code migration plan, stabilization support model and deployment plan in the format proscribed by PG&E's ITM.	— Collibra user run book — Code migration plan, stabilization support model, and deployment plan

Project 2 – DLP Expansion for Unstructured Data

This scope of this project is expansion of DLP scanning activities at PG&E to include on premise unstructured data in multiple repository locations.

This project will help achieve this goal by performing the following:

- Scan and identify PG&E on premise unstructured repositories across PG&E's Customer Care and HR lines of business (Customer Care and HR).
- Obtain access to identified repositories and connect Symantec DLP to identified repositories.
- Scan identified repositories to identify Restricted and Confidential data.
- Update Collibra tool with findings to facilitate identification of security gaps and remediation.
- Prepare maintenance playbook and to the PG&E DLP IT maintenance and operations team.

The table below summarizes our anticipated phases, activities and deliverables for Project 2:

PROJECT 2		
Phase	**Activities**	**Deliverables**
Identify Unstructured Data Repositories	— Draft the following PG&E ITM project deliverables using PG&E ITM templates: • Revised project scope and charter, project work plan, and project job estimate • Unstructured DLP use cases and requirements document. — Create an inventory in excel of HR and Customer Care on premise unstructured repositories (SharePoint, file shares, Documentum, and email) that will be scanned for Confidential and Restricted data	— Revised project scope and charter, project work plan, and project job estimate — Unstructured DLP use cases and requirements document — Stakeholder impact assessment, and change engagement plan

PROJECT 2		
Phase	**Activities**	**Deliverables**
	— Provide guidance to PG&E team members to detect unstructured repositories on the PG&E network. — Compare identified repositories with results from the top-down interview and survey-based approach conducted in Project 1 — Draft standard operating procedure for compiling and maintaining database of on premise unstructured repositories	— Inventory of on premise unstructured repositories to scan — Standard operating procedure for compiling and maintaining database of on premise unstructured repositories
Configure and Test Symantec DLP for Unstructured Data Scans	— Populate Symantec DLP with EDM data and update / configure scanning policies where appropriate — Collaboratively develop detailed application design for deployment of on premise unstructured data scanning capabilities — Conduct functional test on non-production drive shares, SharePoint, and Documentum instances to test EDM scans - Test connectivity to on premise unstructured repositories - Test on premise unstructured repository scan to help ensure Symantec is identifying on premise unstructured Confidential and Restricted data and triggering events; analyze and remediate any false positives - Test system impact of on premise unstructured repository scan	— Updated Symantec DLP policies for on premise unstructured data — Revised performance test plan — Test results
Deploy Test Policies to Production Environment	— Draft the following PG&E ITM project deliverables using PG&E ITM templates: • Prepare the go/no go checklist to evaluate whether the tool's updated functionality can be moved into production — Coordinate with PG&E staff to move Symantec DLP on premise unstructured repository scanning targets and policies from test instance to production instance — Scan on premise unstructured data through phased rollout:	— Scan results for Customer Care and HR on premise unstructured repositories (documented in spreadsheet) — Data-at-rest scanning playbook — Go/no go checklist — Scan results for Customer Care and HR on premise

PROJECT 2		
Phase	**Activities**	**Deliverables**
	- SharePoint, - Drive shares, and - Documentum — Update Collibra tool with metadata obtained from data scanning exercises	unstructured repositories (documented within Collibra)

Project 3 – DLP Expansion for Cloud

The scope of this project is to define PG&E's cloud-based data security approach, key capabilities, and relevant controls based on industry frameworks and leading practices.

This project will help achieve these goals by performing the following:

- Perform a gap analysis of the current state and desired future state of PG&E's cloud-based data security capabilities.
- Define cloud-based data security requirements and integrate them into PG&E standards and policies as required
- Design a solution blueprint that illustrates the ability to enforce data security requirements in the cloud.
- Determine whether extending existing Symantec DLP capabilities (if necessary) into cloud environments may be required to meet data security requirements
- Prepare maintenance playbook and to the PG&E DLP IT maintenance and operations team.

The following table summarizes our anticipated phases, activities, and deliverables for Project 3:

PROJECT 3		
Phase	**Activities**	**Deliverables**
Perform Cloud Capability Gap Analysis	— Draft the following PG&E ITM project deliverables using PG&E ITM templates: • Revised project scope and charter, project work plan, and project job estimate — Perform a gap assessment of current PG&E DLP capabilities in the internal and public cloud — Review and provide recommendations/ updates to standards and policies related to scanning and securing data-at-rest in PG&E's internal and public cloud — Present gap analysis and recommendations to PG&E key stakeholders, and develop a	— Revised project scope and charter, project work plan, and project job estimate — Cloud DLP capability gap analysis and future state recommendations — Suggested revisions to PG&E standards and policies related to scanning and securing data-at-rest in PG&E's internal and public cloud — Design patterns that provide high level

PROJECT 3		
Phase	**Activities**	**Deliverables**
	roadmap for recommended capability enhancements — Provide design patterns for recommended implementation to achieve the key security capabilities required for the future state — Provide design recommendations to policies that can be used to scan cloud-based unstructured data based on existing Symantec DLP deployment	guidance for establishing cloud security capabilities
Configure and Test Symantec DLP for Cloud Data Scans	— Build policies in Symantec DLP (or chosen PG&E solution) to monitor business approved locations of cloud unstructured data — Perform testing of DLP policies, use cases, and scan destination types with sample Personally Identifiable Information (PII) test files with common use cases in the cloud environment — Classify policy response rule actions as block, quarantine, or allow but notify based on severity of incident	— Spreadsheet that identifies up to ten (10) recommended DLP policies that can be used with existing DLP capabilities to mitigate identified cloud risks — Up to ten (10) DLP policies, based on recommendation, configured within the Symantec tool — Test plan based on known data loss use cases and report of policy accuracy metrics with additional recommendations to reduce false positives Recommendations for enforcement actions based on functional testing of DLP policies
Deploy Test Policies to Production Environment	— Coordinate with PG&E staff to move Symantec DLP test instance cloud-based scanning targets and policies to production instance — Scan identified cloud environments through phased rollout — Update Collibra tool with metadata obtained from data scanning exercises	— Technical run book, including revised system architecture diagrams, key configuration items, and report of ongoing system maintenance requirements (if any) — Report detailing DLP policy test results and recommendations for future improvements

Project 4 – De-identification Tool Deployment for Unstructured Data (2019) and Cloud Environments (2020)

The KPMG team will combine data de-identification tool deployment efforts in 2019 and 2020 into one project.

This project will help achieve these goals by performing the following:

- Evaluate current state infrastructure to de-identify and protect data in on-premise unstructured and cloud environments and develop infrastructure deployment plans.
- Define data protection and de-identification requirements for Restricted and Confidential data in production on premise and cloud environments.
- Support expansion of de-identification capabilities to cover on-premise unstructured and cloud environments.

The following table summarizes our anticipated phases, activities, and deliverables for Project 4:

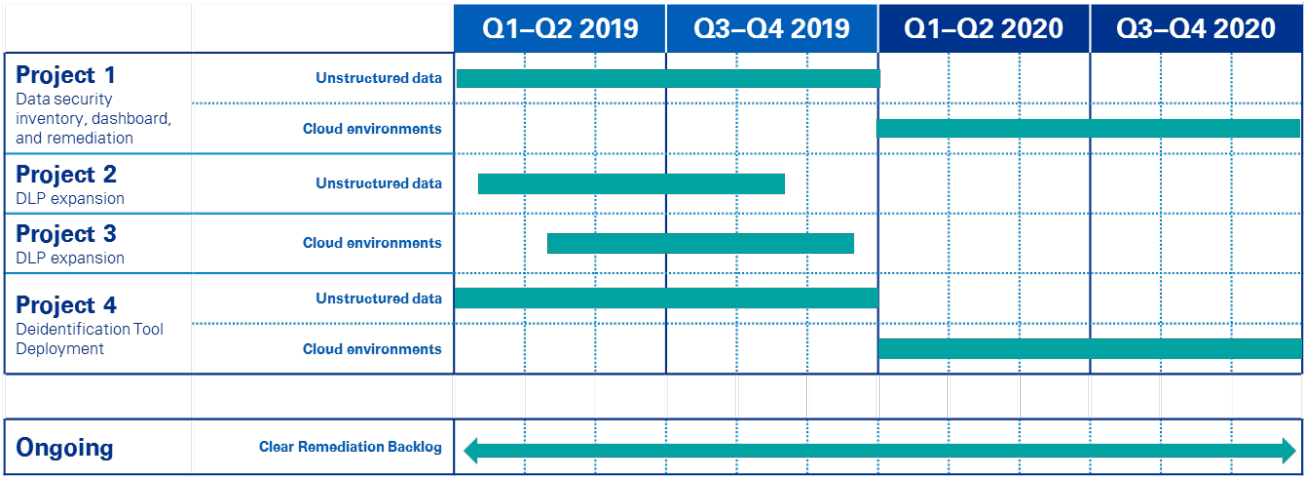
PROJECT 4		
Phase	**Activities**	**Deliverables**
Current State Analysis of De-Identification Tool Deployment	— Draft the following PG&E ITM project deliverables using PG&E ITM templates: • Revised project scope and charter, project work plan, and project job estimate — Perform de-identification scope assessment for production environments to quantify the number of unstructured (2019) and cloud (2020) repositories in scope for de-identification implementation — Prepare deployment methodology recommendations for implementing selected de-identification tool in structured and unstructured environments (2019) and cloud (2020). — Collaborate with Privacy team to identify the exact de-identification requirements and to define Confidential and Restricted data and incorporate results into deployment plan — Review results of 2018 de-identification product deployment project, and integrate lessons learned and product capability list into capability gap analysis. (2019 and 2020) — Identify and select potential locations for on premise unstructured data (2019) and cloud-based (2020) environments — Analyze suitability of de-identification product capabilities for each environment, and provide a prioritized list of suitable / functional capabilities required on premise unstructured data (2019) and cloud-based (2020) environments	— Revised project scope and charter, project work plan, and project job estimate — De-identification scope assessment for production environments and production deployment methodology recommendations — List of selected data repositories, storage types, and locations for de-identification use case testing

PROJECT 4		
Phase	**Activities**	**Deliverables**
	—	
Design Deployment Strategy for Unstructured Data and Cloud Environments	— Create a project plan for re-configuration and extension of selected de-identification product for on premise unstructured data (2019) and cloud-based (2020) environments — Provide a list of suggested configurations for de-identification of data in on premise unstructured data (2019) and cloud-based (2020) environments	— Project plan to modify de-identification product to work with on premise unstructured data , 2019; cloud 2020 — High-level product configuration suggestions for on premise unstructured data 2019; cloud 2020
Support PG&E Configuration of De-Identification Tool to De-Identify Unstructured and Cloud-Based Data	— Assist PG&E with de-identification product reconfiguration effort for on premise unstructured data (2019) and cloud-based (2020) in the PG&E test environment based on developed project plans and provide assistance as needed — Provide a list of observations and issues regarding the completion of the project key success factors — Perform testing of de-identification product configurations, use cases, and scan destination types with sample PII test files and identified use cases in the cloud environment — Deploy changes to de-identification product in test environment to on premise unstructured data (2019) and cloud-based test environments (2020) — Provide requirements for maintenance of the de-identification software outside of normal maintenance activities	— De-identification project configured in test environment to de-identify on premise unstructured data 2019; cloud data 2020. — Test plan based on known data leakage use cases and report of configuration accuracy metrics with additional recommendations — Technical run book, including revised system architecture diagrams, key configuration items, and report of ongoing system maintenance requirements (if any) — Report detailing de-identification test results and recommendations

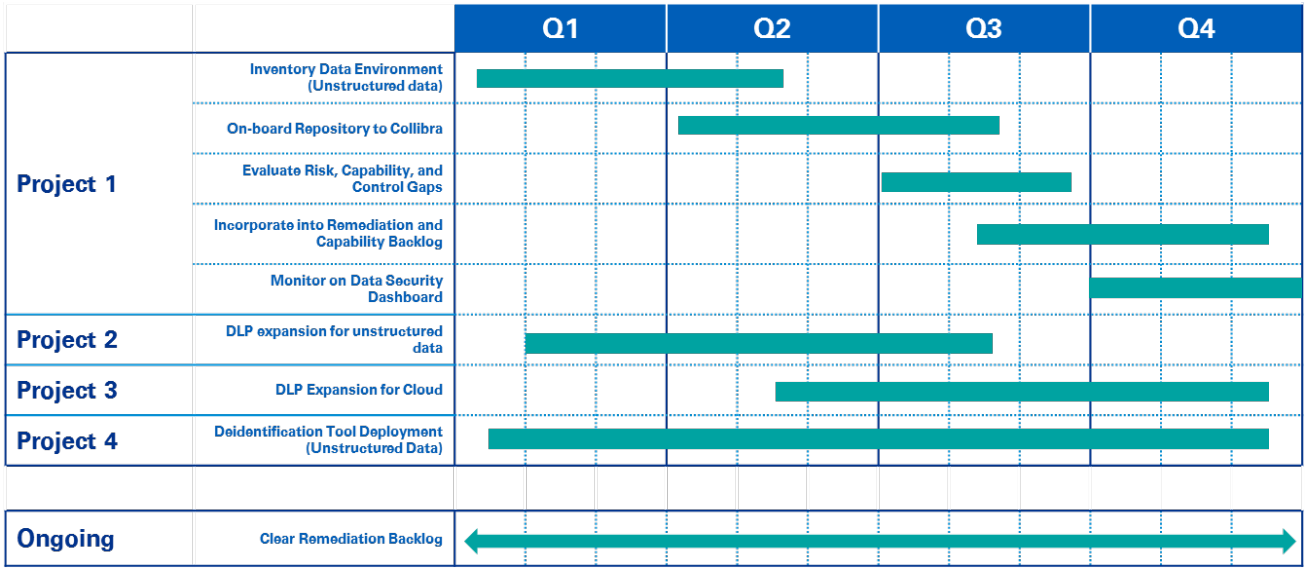
PROJECT 4		
Phase	**Activities**	**Deliverables**
		for future improvements outside of project

4. Project Timelines

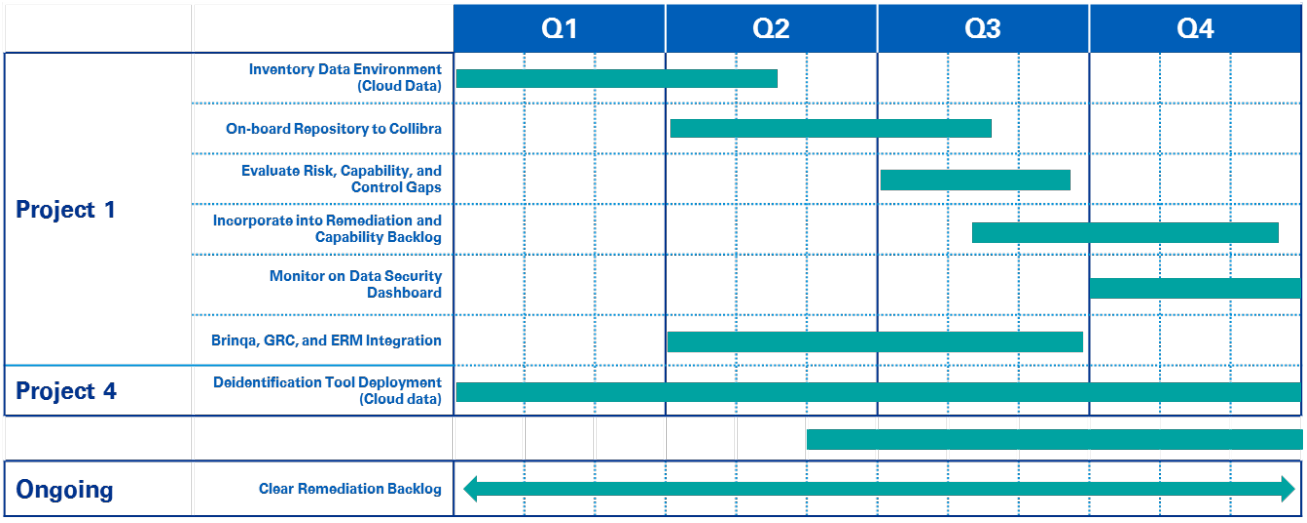
2019–2020 Data Security Project Master Timeline



2019 Projects Detailed Timeline



2020 Projects Detailed Timeline



5. Engagement Fee Schedules

KPMG shall invoice PG&E for a fixed fee of $2,362,456.50 ($1,622,802 in 2019 and $739,654.50 in 2020) plus expenses. Expenses will be billed at actual cost, not to exceed $342,557 ($235,307 in 2019 and $107,250 in 2020) with the approval of PG&E for the delivery period from January 1, 2019 to December 21, 2020. Each payment will be made upon PG&E's review and acceptance of deliverables from each of the activities and will be paid by PG&E within sixty (60) days of receiving a correct invoice. The payment schedule will be as follows:

YEAR	Project	LINE ITEM	MILESTONE	VALUE ($USD)
2019	1. Data Security inventory, dashboard and remediation for on premise unstructured data	1	Revised project scope and charter, project work plan, and project job estimate	$ 32,355.60
		2	Populated on premise unstructured data inventory with associated data classification and extract of data inventory documented in Collibra for structured and unstructured data	$ 48,533.40
		3	Change engagement plan	$ 32,355.60
		4	Collibra use cases and requirements document	$ 40,444.50
		5	Configuration management plan	$ 32,355.60
		6	Disaster recovery plan	$ 24,266.70
		7	Data inventory maintenance playbook and data remediation playbook	$ 48,533.40
		8	Performance test plan	$ 24,266.70
		9	Data security gap assessment for minimum 10 repositories (on premise unstructured data)	$ 40,444.50
		10	Detailed remediation work plans for two to four (2-4) repositories (on premise unstructured data)	$ 32,355.60
		11	Two to four (2-4) repositories remediated in pilot (on premise unstructured data)	$ 32,355.60

		12	Updated data inventory remediation playbook (on premise unstructured data)	$	32,355.60
		13	Test results and disaster recover exercise report	$	32,355.60
		14	Collibra user run book	$	40,444.50
		15	Code migration plan, stabilization support model, and deployment plan	$	32,355.60
			Project 1 - 2019 Total	**$**	**525,778.50**
2019	**2. DLP expansion for on premise unstructured data**	1	Revised project scope and charter, project work plan, and project job estimate	$	14,082.00
		2	Unstructured DLP use cases and requirements document	$	7,041.00
		3	Stakeholder impact assessment, and change engagement plan	$	14,082.00
		4	Inventory of on premise unstructured repositories to scan	$	21,123.00
		5	Standard operating procedure for compiling and maintaining database of on premise unstructured repositories	$	21,123.00
		6	Updated Symantec DLP policies for on premise unstructured data	$	21,123.00
		7	Revised performance test plan	$	14,082.00
		8	Test results	$	7,041.00
		9	Scan results for Customer Care and HR on premise unstructured repositories (documented in spreadsheet)	$	21,123.00
		10	Data at rest scanning playbook	$	21,123.00
		11	Go/no go checklist	$	7,041.00
		12	Scan results for Customer Care and HR on premise unstructured repositories (documented in Collibra)	$	21,123.00
			Project 2 - 2019 Total	**$**	**190,107.00**
2019	**3. DLP expansion for cloud**	1	Revised project scope and charter, project work plan, and project job estimate	$	32,191.00
		2	Cloud DLP capability gap analysis and future state recommendations	$	64,382.00
		3	Suggested revisions to PG&E standards and policies related to scanning and securing data-at-rest in PG&E's internal and public cloud	$	32,191.00
		4	Design patterns that provide high level guidance for establishing cloud security capabilities	$	48,286.00
		5	Spreadsheet that identifies up to ten (10) recommended DLP policies that can be used with existing DLP capabilities to mitigate identified cloud risks	$	48,286.00
		6	Up to ten (10) DLP policies, based on recommendation, configured within the Symantec tool	$	32,191.00
		7	Test plan based on known data loss use cases and report of policy accuracy metrics with additional recommendations to reduce false positives	$	32,191.00
		8	Recommendations for enforcement actions based on functional testing of DLP policies	$	32,190.00

		9	Technical Run book, including revised system architecture diagrams, key configuration items, and report of ongoing system maintenance requirements (if any)	$ 32,191.00
		10	Report detailing DLP policy test results and recommendations for future improvements outside of project	$ 48,289.50
			Project 3 - 2019 Total	**$ 402,388.50**
2019	**4. De-identification tool deployment for on premise unstructured data**	1	Revised project scope and charter, project work plan, and project job estimate	$ 42,044.00
		2	De-identification scope assessment for production environments and production deployment methodology recommendations	$ 84,088.00
		3	List of selected data repositories, storage types, and locations for de-identification use case testing.	$ 42,044.00
		4	Project plan to modify de-identification product to work with on premise unstructured data	$ 42,044.00
		5	High-level product configuration suggestions for on premise unstructured data	$ 63,066.00
		6	De-identification project configured in test environment to de-identify on premise unstructured data 2019; cloud data 2020.	$ 63,066.00
		7	Test plan based on known data leakage use cases and report of configuration accuracy metrics with additional recommendations	$ 31,533.00
		8	Test results	$ 63,066.00
		9	Technical run book, including revised system architecture diagrams, key configuration items, and report of ongoing system maintenance requirements (if any)	$ 31,533.00
		10	Report detailing de-identification test results and recommendations for future improvements outside of project	$ 42,044.00
			Project 4 - 2019 Total	**$ 504,528.00**
			2019 Total	**$1,622,802.00**

YEAR	PROJECT	LINE ITEM	MILESTONE	VALUE ($USD)
2020	**1. Data Security inventory, dashboard and remediation for cloud environment**	1	Revised project scope and charter, project work plan, and project job estimate	$ 32,355.60
		2	Populated data inventory with associated data classification and extract of data inventory documented in Collibra for cloud data (2020)	$ 48,533.40
		3	Change engagement plan	$ 32,355.60
		4	Collibra use cases and requirements document	$ 40,444.50
		5	Configuration management plan	$ 32,355.60

		6	Disaster recovery plan	$ 24,266.70
		7	Data inventory maintenance playbook and data remediation playbook	$ 48,533.40
		8	Performance test plans	$ 24,266.70
		9	Data security gap assessment for minimum ten (10) repositories (cloud data)	$ 40,444.50
		10	Detailed Remediation work plans for two to four (2-4) repositories (cloud data)	$ 32,355.60
		11	Two to four (2-4) repositories remediated in pilot (cloud data)	$ 32,355.60
		12	Updated data inventory remediation playbook (cloud data)	$ 32,355.60
		13	Test results and disaster recover exercise report	$ 32,355.60
		14	Collibra user run book	$ 40,444.50
		15	Code migration plan, stabilization support model, and deployment plan	$ 32,355.60
			Project 1 - 2020 Total	**$ 525,778.50**
2020	**4. De-identification tool deployment for cloud environment**	1	Revised project scope and charter, project work plan, and project job estimate	$ 17,823.00
		2	De-identification scope assessment for production environments and production deployment methodology recommendations	$ 35,646.00
		3	List of selected data repositories, storage types, and locations for de-identification use case testing	$ 17,823.00
		4	Project plan to modify de-identification product to work with unstructured data	$ 17,823.00
		5	High-level product configuration suggestions for unstructured data	$ 26,734.50
		6	De-identification project configured in test environment to de-identify on premise unstructured data 2019; cloud data 2020.	$ 26,734.50
		7	Test plan based on known data leakage use cases and report of configuration accuracy metrics with additional recommendations	$ 13,367.25
		8	Test results	$ 26,734.50
		9	Technical run book, including revised system architecture diagrams, key configuration items, and report of ongoing system maintenance requirements (if any)	$ 13,367.25
		10	Report detailing de-identification test results and recommendations for future improvements outside of project	$ 17,823.00
			Project 4 - 2020 Total	**$ 213,876.00**
			2020 Total	**$ 739,654.50**

The foregoing fees include a significantly discounted hourly rate which shall satisfy the "Volume Rebate," "Tenure Discount" and "No Bid Discount" provisions set forth in the MSA, such that the fees set shall not be recalculated in the rebate calculations.

PG&E will perform timely review and provide timely sign-off for each KPMG deliverable. Deliverable sign-off will occur and assume within five working days from the submission of deliverables

Contractor will endeavor to notify PG&E if the Contractor professionals encounter unexpected circumstances that warrant additional time or expense, or a modification of the scope of the engagement. If such circumstances require a modifications, the Contractor will discuss the impact of such circumstances with PG&E, mutually agree on any modification, and issue a Change Order to the approve SOW, to confirm the understanding

KPMG acknowledges that the Bankruptcy Court must approve its fees in order to be compensated. In that regard, KPMG intends to file applications with the Court for allowance of compensation and reimbursement of expenses in accordance with the Bankruptcy Code, the Bankruptcy Rules, the Local Bankruptcy Rules, and any order of the Bankruptcy Court establishing procedures for monthly compensation and reimbursement of expenses for professionals. The Company acknowledges that professional time required to prepare detailed applications in accordance with the Bankruptcy Code, applicable rules and guidelines differs from KPMG's normal billing procedures and, as a result, requires significant effort by KPMG to comply therewith. The expense required by this effort was not included in the estimated fees described above. The Company agrees that, subject to Bankruptcy Court approval, KPMG shall be reimbursed for such professional time incurred.

To the extent that the services involve procedures in connection with the company's restructuring activities or emergence from bankruptcy, such work will be considered out-of-scope services under the engagement letters ("Out-of-Scope Services"). Such Out-of-Scope Services also include professional time required to prepare detailed applications in accordance with the Bankruptcy Code (described above). To the extent that changes in circumstances, such as the loss of Company personnel during the bankruptcy process, increase the effort required to deliver the services, this additional effort also will be billed as Out-of-Scope Services. Out-of-Scope Services will be billed in addition to the fixed fees described above, at 100% of our standard professional hourly rates. In its fee applications, KPMG will identify and describe any Out-of-Scope Services.

6. Engagement Team

A two year program requires a creative approach to bringing consistency of resources while continually introducing new resources with specialized skills and insights. Knowing how and when to transition resources will be imperative to meeting the program objectives while helping to achieve the aggressive affordability goals for 2019 and beyond.

The following team of KPMG professionals will provide the highest quality of professional services as needed by the PG&E, as outlined below -

- **Michael Gomez (Engagement Partner):** Michael will be responsible for overseeing the overall quality of service PG&E receives from KPMG and is available as a source of escalation as needed.
- **Toby Sedgewick (Engagement Manager):** Toby's responsibilities include: managing resources, tracking budget, creating and overseeing schedules, tracking issues and risks, reporting to management as requested.
- **Josh Conkel (Technical Lead):** Josh will be responsible for leading the resources who will be executing the technical requirements as noted in the approach stages above.
- **Other Subject Matter Professionals:** This engagement will be staffed by qualified and experienced professionals who will work as a team designed to meet PG&E's needs. In addition to the aforementioned professionals, KPMG will leverage a combination of skilled resources to execute the engagement. Over the course of the project, the following resources will be on-boarded when appropriate to support project activities:

- A resource experienced in Collibra solution design that will work collaboratively with PG&E Data Governance team to support the design and configuration of the Collibra expansion to meet the data security program's use cases;
- An experienced de-identification resource that has knowledge of unstructured and cloud de-identification methodologies and can support the expansion and configuration of the selected de-identification tool to de-identify these environments;
- An experienced DLP solution analyst who will develop policies, including preparing target connection strings and associated DLP policies, for detection of restricted and confidential data in unstructured and cloud environments. Analyst will also have experience analyzing scan results for improvement opportunities, and will have SQL skills to design queries to build exact data match indexes;
- An offshore analyst that will support project management and coordination activities.

7. Other Matters

KPMG will provide our services in accordance with the terms and conditions of this SOW. Our services as outlined in this letter constitute an Advisory Engagement conducted under the American Institute of Certified Public Accountants ("AICPA") Standards for Consulting Services. Such services are not intended to be an audit, examination, attestation, special report or agreed-upon procedures engagement as those services are defined in AICPA literature applicable to such engagements conducted by independent auditors. Accordingly, these services will not result in the issuance of a written communication to third parties by KPMG directly reporting on financial data or internal control or expressing a conclusion or any other form of assurance.

The Deliverables presented as part of this engagement are for the internal use of PG&E management, the Audit Committee, and Board of Directors and are not to be distributed externally to third-parties, in whole or in part, without prior written consent from Contractor in each instance, or used for any other purpose. Contractor disclaims any intention or obligation to update or revise the observations whether as a result of new information, future events or otherwise. Should additional documentation or other information become available which impacts upon the observations described in the Deliverables, Contractor reserves the right to amend its observations and summary documents accordingly.

PG&E consents to Contractor's disclosure to a member firm, affiliate or third party service provider and such member firms, affiliates and third party service provider's use of data and information, including but not limited to Confidential Information.

Contractor is responsible for ensuring that any member firm, affiliate or third party service provider to whom Contractor shares PG&E's data or information uses such data or information in way that is no less protective of the data or information than Contractor has agreed to, and only for the purposes set forth in this Agreement.

Any Services performed by a member firm, affiliate or third party service provider shall satisfy the terms of this Agreement and the applicable SOW and Contractor shall remain responsible to PG&E for the performance of such Services. PG&E agrees that any claim relating to the Services may only be made against Contractor and not any other member firm, affiliate or third-party service provider referred to above.

Contractor will act as an independent contractor in providing the services as set out in this SOW and does not undertake to perform obligations of PG&E, whether regulatory or contractual. In carrying out our work hereunder:

- Contractor will provide its services in accordance with the terms and conditions of this SOW and the MSA No. 4400011340. Contractor will not act in the capacity equivalent to a member of management or as an employee of PG&E
- Contractor will provide observations to PG&E management during this engagement. PG&E management is solely responsible for evaluating such observations and then determining what changes/improvements (if any) PG&E should implement in light of PG&E's objectives in carrying out the project to which Contractor's services relate (the "Project")
- Contractor will not form part of the PG&E's internal control structure

Conflicts of Interest

- PG&E agrees that it will inform KPMG of the technology vendors ("parties") to be evaluated. At such time, KPMG will perform a limited internal search for relationships on those parties.
- If identified, KPMG will advise PG&E of the general nature of any services provided by KPMG, or other member firms of the KPMG network of independent firms and firms and entities controlled by, or under common control with, one or more such member firms (collectively, "Member Firms") to the parties (i.e., audit, tax and/or advisory).
- If PG&E fails to promptly notify KPMG of its objection to any identified relationships, PG&E agrees that the identified relationships do not (i) constitute a limitation on the services requested, (ii) create a basis for disqualification of KPMG or its professionals, or (iii) constitute a conflict of interest for purposes of KPMG's engagement to perform the services for PG&E. PG&E expressly waives its right to assert any such conflict against KPMG.
- KPMG's process for conducting searches of potential conflicts takes place at the time the parties are identified and provided by PG&E. However, if KPMG becomes aware of any potential conflicts after the start of the engagement, KPMG will promptly inform PG&E. In addition, during the course of this engagement, PG&E agrees that they will inform KPMG of additional parties in this matter or name changes for those parties previously provided. At such time, KPMG will perform an additional limited internal search for relationships on those parties. If identified, KPMG will advise PG&E of the general nature of any services provided to that subject (i.e., audit, tax and/or advisory).
- KPMG reserves the right to resign from this engagement at any time if a conflict, as contemplated by the professional standards of the AICPA, law or regulation, arises or becomes known to KPMG that prohibits KPMG from conducting this engagement, or in KPMG's judgment, would impair KPMG's ability to perform objectively. If KPMG serves as independent auditors of a party, KPMG may require consent from the party, which will be determined on a case-by-case basis.

8. Systems Implementation

The systems implementation terms attached in Appendix A: Systems Implementation Addendum to Master Professional Services Agreement are incorporated into this SOW by this reference.

9. Engagement Assumptions

The success of this project is highly dependent on project coordination and support from PG&E. Contractor's services described in this document are per following assumptions:

- PG&E will assume overall responsibility for this project.
- PG&E will designate a management level individual as a coordination point and who will facilitate the scheduling of interviews and working sessions, the gathering of documentation and information supporting analysis conducted.
- PG&E will also identify a project owner for this project who will be available for review and approval of deliverables. If changes in PG&E personnel result in the delay or change of milestones under this SOW, Contractor and PG&E will meet, determine the impact and the appropriate course of action, which may include, but not be limited to modifying the level of Contractor resources (and modification of Contractor fees, in a manner consistent with this SOW)
    - The PG&E project owner will oversee the conduct of this project, including coordination of PG&E resources needed.
    - The PG&E project owner will maintain an effective internal communication and control structure. The responsibility for establishing and maintaining adequacy of the controls in place over security and directing activities related to the review of business processes and controls rests with management of PG&E project owner.
    - The PG&E project owner will establish the project objectives, scope and extent of Contractor services. The project scope will be agreed upon by both PG&E, and the Contractor team and will not change without the prior written approval of both parties.
    - The PG&E project owner will oversee, along with the Contractor team, the project progress and address issues as they arise.
    - The PG&E project owner assigned to the project will review draft deliverables on a timely basis. PG&E will provide timely sign-off for each project stage. Deliverable sign-off will occur and assume within five working days from the submission of deliverables.
- PG&E will be responsible for staffing a Data Security Program Office with sufficient resources to operationalize project activities beyond the scope of this SOW.
- PG&E will be responsible for staffing the Data Security Program with appropriate resources to support project work. These resources will be identified in the Deliverable Responsibility Matrix (DRM) for each project that will be created during each projects planning phase, in accordance with PG&E's IT Methodology (ITM). This will include a full-time project manager who will manage PG&E project financials, identify and onboard internal PG&E project resources, have final responsibility for PM associated ITM deliverable approvals, have final responsibility for socialization of all deliverables, and will serve as the primary point of contact for invoicing. Additionally, PG&E will assign a solution architect to each project who will be responsible for deliverable creation and socialization of all solution architect deliverables. PGE will assign sufficient resources to complete all additional IT Methodology deliverables in a timely manner. Examples of these resources include a, IT service introduction lead, a disaster recovery lead, and a cybersecurity risk advisor. PG&E will contract directly with any vendors whose tools or products that KPMG will be using, configuring, or implementing as part of this SOW.

- PG&E will make any and all management decisions related to the scope of this project.
- KPMG services provided as part of this project are limited to the project scope, and will not act as a direct employee or agent of PG&E.
- KPMG will provide observations and suggest recommendations to PG&E management during the course of this engagement. PG&E staff (management and employees) is solely responsible for evaluating and deciding what recommendations are accepted and should be put in place.
- PG&E will provide appropriate workspace for the Contractor resources when on-site, including, but not limited to, telephones, workstations, printers, whiteboards, office supplies, photocopiers, internet access, and fax machines.
- PG&E will work with Contractor to resolve any and all issues related to the project in a timely fashion.
- It is assumed that PG&E will provide timely sign-off for each project phase. Deliverable sign-off will occur and assume within five working days from the submission of deliverables. The responsibility for the Project rests with management of PG&E. With regard to Contractor's services, PG&E is responsible for:
    - Determining the objectives, scope, and extent of Contractor's services hereunder
    - Designating a management-level individual, who will have responsibility to manage and oversee, as assisted by the Contractor team, the Project progress and to address issues as they arise, and who has the skills and experience necessary to effectively perform this function, including but not limited to:
        - Familiarity with the business functions, processes or divisions that are the subject of the Project objectives;
        - Being in a position to evaluate the information provided to him/her by the Contractor engagement team; is responsible for, and authorized to make management decisions based on such information; and
        - In a sufficiently senior position, or to otherwise have a reporting relationship with senior management to provide appropriate internal PG&E communications regarding project status and potential concerns.
    - Agreeing to a written management framework that identifies PG&E managers responsible for approvals and judgments and for approving key milestones and interim and final deliverables as defined by PG&E
    - Evaluating the adequacy of the procedures performed by Contractor
    - Evaluating the observations and recommendations arising from Contractor's services contemplated by this SOW
- PG&E gives Contractor the right to use PG&E's logo on documents prepared for PG&E internally (e.g., internal presentations, etc.) and for no other purpose.

Scope changes that are agreed upon by both PG&E and KPMG, and will not change without the prior approval from both parties. If required, a change order will be submitted to update the milestones and/or deliverables.

Technical Assumptions

- PG&E will provide KPMG access to their personnel and facilities sufficient for KPMG to fulfill its obligations under this proposal. This includes (but is not limited to):
    - Providing necessary computing resources including all hardware, software, licensing (where applicable), and access required for discovery, reporting, and monitoring activities described in this document. PG&E will install and implement all necessary hardware and software necessary for the completion of the project, including backend services such as databases, servers, firewalls, and networks.
    - Granting remote access to the PG&E development, test, and production environments through the use of Citrix Terminal Server or Citrix Virtual Desktop (if tools require a workstation).
    - KPMG will not be responsible for delays in the selection of the data de-identification tool or contracting and licensing agreements. KPMG and PG&E team will work together on any impacts to the timelines and deliverables due to the delays. If required, a change order will be submitted to update the milestones and/or deliverables.
- Allocating appropriate workspace for the KPMG resources on-site, such as telephones, workstations, printers, whiteboards, office supplies, photocopiers, internet access, and fax machines.
- PG&E will be responsible to fix any project related product's defects, and KPMG will not be responsible for performance of troubleshooting of server-level infrastructure issues for production systems.
- KPMG will not be responsible for data cleansing beyond the initial cleansing performed as explicitly defined in this SOW.
- KPMG will only work on non-production environment(s) of Symantec DLP and the de-Identification tool. KPMG will assist with PG&E's migrations of Symantec DLP, de-identification, and Collibra changes into the production environment by following PG&E's change management processes.
- All non-production environments (applications, servers, systems, databases, etc.) will be available (up and running normal) and accessible during the duration of this engagement. Any planned downtime will be communicated in advance to KPMG. Some unplanned downtimes are expected. PG&E and KPMG will work together on potential impact to the timelines due to any delays due to unavailability.
- PG&E will be responsible for Data de-identification tool patching, maintenance and operations for both non-production and production environments.

Scoping Assumptions

- One (1) engagement kick-off meeting to be held in 2019 and 2020.
- One (1) or two (2) weekly status meetings to be held to provide updates on project status. Weekly status meetings will cover all or a select group of projects as agreed with project stakeholders.
- Project scope will be limited to repositories and data associated with the Customer Care and Human Resources Lines of Business.

Project 1. Data Security inventory, dashboard and remediation for on premise unstructured data / within cloud environment

- For the stakeholder interviews to be held to populate on premise unstructured data inventory, projected effort is twenty-five (25) to thirty (30) interviews.

- For the stakeholder interviews to be held to populate cloud data inventory, projected effort is twenty-five (25) to thirty (30) interviews.
- For the stakeholder interviews to be held to agree on premise unstructured data repository remediation plans, projected effort is ten (10) to fifteen (15) interviews.
- For the stakeholder interviews to be held to agree cloud data repository remediation plans, projected effort is ten (10) to fifteen (15) interviews.
- PG&E team members will perform infrastructure build work and support project team to configure Collibra to facilitate the data security program's use case of Collibra, as defined in the approach section above.
- PG&E team will secure Business Owner cooperation and participation in remediating target repositories that have been observed to have security gaps.

Project 2. DLP expansion for on premise unstructured data

- PG&E team members will use PG&E tools to detect SharePoint, network shared drives, and Documentum instances on PG&E network. PGE team members will perform these activities within a timeline defined during execution of the project.
- PG&E team members will provision a DLP scanner account on each repository with sufficient access to scan each of the identified-on premise unstructured repositories within eight weeks (8) of KPMG requesting access. Any repositories that have not been provisioned sufficient access within eight (8) weeks will not be included in the scope of this SOW.
- PG&E team members will review, approve, and coordinate movement of DLP policies from test environment to production environment.

Project 3. DLP expansion for cloud data

- PG&E team members will select, test, and implement in production a Cloud Access Security Broker (CASB).
- PG&E team members will provision a DLP scanner account on each repository with sufficient access to scan each of the identified unstructured repositories within eight weeks (8) of KPMG requesting access. Any repositories that have not been provisioned sufficient access within eight (8) weeks will not be included in the scope of this SOW.
- PG&E team members will review, approve, and coordinate movement of DLP policies from test environment to production environment.

Project 4. DLP expansion for unstructured data and cloud environments

- PG&E has already purchased and implemented a de-identification tool that can be leveraged for cloud and unstructured data. If a new tool is required, PG&E will select and purchase a tool by June 30, 2019.

Enclosure: Appendix A – System Implementation Addendum to Master Professional Services Agreement

ATTACHMENT 2 - Appendix A

Systems Implementation Addendum to
Master Professional Services Agreement

This SI Addendum ("**SI Addendum**") is made and entered into by and between PG&E ("**PG&E**") and KPMG LLP ("**Consultant**") and amends the Services Agreement ("**Agreement**"), incorporated by reference into the statement of work executed by and between PG&E and Consultant (the "**SOW**"). In the event of a conflict between (on the one hand) the provisions of this SI Addendum and (on the other hand) the provisions of the SOW and Agreement, this SI Addendum will govern with respect to the system implementation services described in the SOW ("**SI Services**"). Any capitalized term not otherwise defined in this SI Addendum will have the meaning ascribed to it in the SOW or the Agreement (as applicable).

1. **Definitions**. "**PG&E Materials**" shall mean any and all materials, facilities, network, hardware, systems, software, data and other equipment or information, owned by or licensed or leased to PG&E (including any Third Party Materials (as defined in Paragraph 3(d) below)), to which Consultant is provided with access in connection with the SI Services and which may be used by Consultant in providing the SI Services, Deliverables and/or Configured System pursuant to the SOW. "**Configured System**" means the Third Party Materials as configured by the SI Services. "**Consultant Knowledge**" includes, in addition to the items enumerated in Section 16 of the Agreement, the following materials and project tools: (i) components, programs, systems, analysis, frameworks, documentation, drawings, configuration techniques and specifications, owned by or licensed or leased to Consultant or any of the other Consultant Parties, and (ii) any modifications, enhancements, improvements or derivative works of any Consultant Knowledge, irrespective of their date of creation.

2. **Use of PG&E Materials and Acceptance.**

   a. With respect to any PG&E Materials to which Consultant is provided with access in connection with the SI Services, PG&E hereby grants to Consultant a non-exclusive, transferable, sublicensable, paid-up, royalty-free right and license to use, copy, modify and make derivative works of, and transmit such PG&E Materials to the extent necessary for Consultant to provide the SI Services to PG&E.

   b. Upon delivery of a Deliverable or Configured System to PG&E, PG&E shall review the Deliverable or Configured System in accordance with the acceptance procedure and within the acceptance period specified in the SOW, or where no such acceptance period is specified, within ten (10) business days of delivery. PG&E may reject the Deliverable or Configured System within the applicable acceptance period by providing to Consultant a notice of rejection ("**Rejection Notice**") specifying a list of material non-conformities with the specifications set forth in the SOW (the "**Specifications**"). To be effective, the Rejection Notice shall be in writing (email being acceptable) and sent to the Consultant Project Manager specified in the SOW or otherwise identified to PG&E in writing by Consultant. Consultant shall then conform the Deliverable or Configured System to the Specifications and resubmit it to PG&E for review and acceptance in accordance with this Paragraph 2(b). This process will continue until the Deliverable or Configured System is accepted under this Paragraph 2(b). The Deliverable or Configured System will be accepted when the applicable acceptance period has expired without Consultant receiving an effective Rejection Notice, or when PG&E uses such Deliverable or Configured System (notwithstanding any rejection of such Deliverable or Configured System) in a production environment, whichever occurs first.

3. **Warranties and Disclaimers.**

   a. Consultant warrants to PG&E that (i) Consultant will provide the SI Services using reasonable care and skill, and (ii) for a period of ninety (90) days after acceptance thereof, each Deliverable or Configured System as delivered by Consultant will conform to its Specifications in all material respects. Any claim for breach of Consultant's warranties in this Paragraph 3(a) with respect to any SI Service, Deliverable or Configured System must be made by written notice to Consultant within thirty (30) days of provision of such SI Service or within ninety (90) days of acceptance of such Deliverable or

Configured System (as applicable). For any such breach, PG&E's exclusive remedies, and Consultant's entire liability, shall be, at Consultant's option, (i) the re-provision of such SI Service, or the repair and replacement of the Deliverable or Configured System (as applicable), or (ii) the refund to PG&E of the amount paid to Consultant for the specific SI Service, Configured System or Deliverable.

b. PG&E represents, warrants and covenants to Consultant that (i) PG&E has obtained all consents, permits, licenses and other approvals required (if any) to grant Consultant the rights under Paragraph 2(a) of this SI Addendum, (ii) Consultant's exercise of its rights under Paragraph 2(a) will not infringe, misappropriate or otherwise violate the rights of any third party (including the rights of any owner of Third Party Materials), or violate any applicable law, rule, regulation or other official government release and (iii) PG&E will use the Configured System in accordance with applicable law.

c. **PG&E UNDERSTANDS THAT CONTRACTOR IS PROVIDING THE SI SERVICES HEREUNDER IN RELATION TO PG&E MATERIALS (INCLUDING THIRD PARTY MATERIALS) FOR WHICH CONTRACTOR HAS NO RESPONSIBILITY. EXCEPT AS EXPRESSLY STATED IN PARAGRAPH 3(a) ABOVE, CONTRACTOR EXPRESSLY DISCLAIMS AND MAKES NO WARRANTIES OF ANY KIND OR NATURE WITH RESPECT TO THE SI SERVICES, PG&E MATERIALS (INCLUDING THIRD PARTY MATERIALS), DELIVERABLES, CONFIGURED SYSTEM OR OTHERWISE, WHETHER EXPRESSLY IN THE SOW OR OTHERWISE EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, OR NON-INFRINGEMENT, OR THE APPROPRIATENESS OF PG&E OR THIRD-PARTY SPECIFICATIONS. IN ADDITION, CONTRACTOR EXPRESSLY DISCLAIMS ANY WARRANTY OR LIABILITY WITH RESPECT TO DESIGN OR LATENT DEFECTS OR COMPLIANCE WITH LAWS, RULES, REGULATIONS, OR OTHER OFFICIAL GOVERNMENT RELEASES APPLICABLE TO PG&E, WHICH SHALL BE THE SOLE RESPONSIBILITY OF PG&E**.

d. The SI Services may include providing assistance to PG&E with PG&E's procurement of third-party hardware, software or other items which will be identified in the SOW (such items, together with all other third party items used or provided in connection with the Work and/or Deliverables provided pursuant to the SOW shall be referred to as the "**Third Party Materials**"). Unless otherwise expressly stated in the SOW, PG&E will license or purchase such Third Party Materials directly from the vendor or reseller (which may be an affiliate of Consultant). PG&E retains sole responsibility for compliance with the license terms governing such Third Party Materials, the selection of such Third Party Materials, and, unless the SOW expressly specifies otherwise, the payment therefor. If Consultant agrees in the SOW or otherwise to provide any Third Party Materials, such THIRD PARTY MATERIALS ARE PROVIDED ON AN "AS IS" "AS AVAILABLE" BASIS WITHOUT WARRANTY FROM CONSULTANT, with the exception of any manufacturers' or licensors' warranties which Consultant is able to arrange for PG&E's benefit. Consultant, its Member Firms, and its and their subcontractors, reserve the right to retain ancillary benefits, including credits, rebates or referral fees, they may receive relating to such Third Party Materials, regardless of whether PG&E pays for such Third Party Materials directly, on a pass-through basis, or otherwise. PG&E agrees that the retention of such benefits shall not constitute a conflict of interest.

4. **Deliverables.** Upon full and final payment by PG&E of all amounts due under the SOW, Consultant hereby grants to PG&E a perpetual, non-exclusive, non-transferable, paid-up, royalty-free right and license to use, copy, modify, make derivative works of, distribute, display and perform the Deliverables or Configured System, and any Consultant Knowledge to the extent embedded therein, solely for PG&E's own internal business purposes and subject to any other restrictions specifically set forth in the SOW; provided that PG&E may provide the Deliverables or Configured System to an affiliate or third party (each, an "**Approved Sublicensee**") solely for purposes of operating, maintaining and enhancing PG&E's internal use of the Deliverables or Configured System in PG&E's business. PG&E shall ensure that each such Approved Sublicensee complies with all applicable terms of this SI Addendum and shall be liable to Consultant for any damages caused by an Approved Sublicensee's failure to do so. Except as expressly provided in this Paragraph 4, PG&E may not sell or license, in whole or in part, the Deliverables or Configured System. Consultant shall own all right, title and interest in and to any Deliverables or Configured System produced under this SI Addendum, including any modifications, enhancements, improvements or derivative works of any PG&E Materials (including modifications, enhancements, improvements or derivative works of any Third Party Materials), whether developed by or on behalf of

Consultant solely or both parties jointly, other than any PG&E Materials incorporated therein, the rights in which shall remain in PG&E (subject to the license to Consultant granted under Paragraph 2(a) above).

5. **Indemnification.** Without limiting Section 28.2 of the Agreement, PG&E shall indemnify, hold harmless and defend the Consultant from and against any and all Liabilities incurred or suffered by or asserted against the Consultant in connection with a third party claim to the extent resulting from (a) the PG&E Materials and/or any other materials provided by or on behalf of any of the PG&E Parties, (b) Consultant's compliance with any designs, specifications, or instructions provided by or on behalf of any of the PG&E Parties, (c) PG&E's breach or alleged breach of Paragraph 3(b) or Paragraph 4 hereof, (d) use by or on behalf of PG&E of any Deliverables or Configured System other than as provided or updated by Consultant, and (e) any unauthorized use of any Deliverables or Configured System in the possession or control of PG&E or any Approved Sublicensee.

6. **Changes and Adjustment Events**.

   a. The parties acknowledge and agree that the occurrence of any of the following events (each, an **"Adjustment Event"**) may require an extension in the schedule set forth in the SOW and/or an increase in the fees and expenses and/or a change to the nature of the SI Services: (i) a change to, deficiency in, or retraction of information or materials supplied to Consultant by or on behalf of any of PG&E; (ii) a failure by PG&E and/or its vendors to perform any of their respective responsibilities in a timely manner, including the supply to Consultant of adequate resources and information; (iii) the failure of any PG&E Materials provided by or on behalf of PG&E to perform in accordance with applicable specifications; (iv) circumstances beyond the reasonable control of Consultant, including actual or potential force majeure events; (v) any assumption in the SOW not being fully realized; or (vi) PG&E's failure to timely obtain pursuant to Paragraph 3(b) above all of the consents, permits, licenses and other approvals necessary for Consultant to provide the SI Services in the manner, and accordance with the schedule, set forth in the SOW.

   b. In the event an Adjustment Event occurs or the parties agree on a change to the scope of SI Services, Consultant may prepare and provide to PG&E a proposed change order identifying the impact and setting forth any applicable adjustments in the schedule and/or payments to Consultant. An authorized representative of each party shall promptly sign each such proposed change order to acknowledge the impact and to indicate that party's agreement to the adjustments.

   c. Notwithstanding Paragraph 6(a) above, if any delays or deficiencies in the SI Services, or with respect to the Deliverables or Configured System, occur as a result of Adjustment Events, the scheduled completion date under the SOW for the affected SI Services, Deliverables and/or Configured System shall be extended to the extent of any such delays or deficiencies, and Consultant shall not incur any liability to PG&E as a result of such delays or deficiencies.